IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

UNITED STATES OF AMERICA	)	
	)	
v.	)	NO.: 3:08-cr-142
	)	JUDGES PHILLIPS/SHIRLEY
	)	
DAVID C. KERNELL	)	

MOTION TO SUPPRESS EVIDENCE FOR WHICH NO PROBABLE CAUSE EXISTED, HAVING BEEN OBTAINED EITHER OUTSIDE THE SCOPE OF AUTHORITY GRANTED BY THE WARRANT OR UNDER THE AUTHORITY OF AN UNCONSTITUTIONAL GENERAL EXPLORATORY WARRANT

Comes the defendant, David C. Kernell, through undersigned counsel and pursuant to Rules 12 and 41 of the Federal Rules of Criminal Procedure and the Fourth Amendment to the U.S. Constitution, and hereby respectfully moves this Court for an Order suppressing the admission of the computer seized from Mr. Kernell's apartment in September 2008 and any information or documents obtained from the off-site forensic search of the computer. When the government seized Mr. Kernell's computer, it seized the entirety of its contents, irrespective of whether a neutral magistrate had found probable cause for the seizure of such materials. The government effectively bypassed the probable cause requirement by claiming that "[s]earching computer systems for criminal evidence can be a highly technical process." See Affidavit in Support of Search Warrant, In the matter of the Search of Room A, 3:08-MJ-1084, 9/20/2008, ¶ 32.

This motion addresses the scope of reasonable searches and seizures of electronic evidence. The bases for this motion are:

(1) The warrant authorized the seizure of a laptop computer and a limited number of its files.

(2) Once seized, the government exceeded the scope of its authority by examining all of the computer's contents without the judicial approval to do so.

(3) At minimum, the government could and should have submitted a search protocol for judicial approval that would have limited all subsequent searches to those files for which there was probable cause.

(4) The only way the warrant could be read to authorize such electronic rummaging through documents and files would transform it into a general warrant.

(5) General warrants are prohibited by the Fourth Amendment to the U.S. Constitution.

(6) If, as the affidavit states, it was not feasible to seek judicial approval of a search protocol before seizing the computer, the Constitution required the government to limit the search after the seizure by seeking judicial approval.

Mr. Kernell does not yet have the reports concerning the forensic analyses performed on his computer or its contents. Therefore, he does not yet know the full extent of the government's intrusion into materials for which there was no probable cause. Mr. Kernell requests an evidentiary hearing on the issues raised in this motion.

In further support of this motion Mr. Kernell submits the following memorandum of law.

I. INTRODUCTION

On September 20, 2008, Special Agent Andrew M. Fisher ("Agent Fisher") of the F.B.I. submitted an application and affidavit for a search warrant to search and seize items from Mr. Kernell's apartment. (Application and Affidavit for Search Warrant, including attachments, In the matter of the Search of Room A, 3:08-MJ-1084, 9/20/2008) Agent Fisher avowed that, "there is probable cause to believe that Governor Palin's e-mail account was compromised in violation of Title 18, United States Code 1030(a)(2)(C) and (c)(2)(B) . . . ." (Affidavit in

Support of Search Warrant ¶ 3). The warrant[1] was signed by the United States Magistrate Judge at 11:17 p.m. and executed at 11:55 p.m. (Search Warrant & Return In the matter of the Search of Room A, 3:08-MJ-1084, 9/20/2008).

Agent Fisher's application to the Court sought permission to seize Mr. Kernell's computer and everything contained within and associated with it. [2] The affidavit stated that

[1] The affidavit was not expressly incorporated into the warrant, though its existence was referenced. If the affidavit was not incorporated, there was no crime listed on the warrant or in the attachments. United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) ("warrants for computers searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material," not followed in this child pornography case); United States v. Gleich, 397 F.3d 608 (8th Cir. 2005) (description of visual representations of "sexual conduct by a minor" sufficient, as such items "specifically prohibited by statute"). Here, by comparison, having an email address or computer is not prohibited. And, as mentioned in one of Mr. Kernell's prior-filed motions, the term "hacking" is not statutorily defined and therefore, even if one knew the meaning of the term, not specifically prohibited by statute and therefore not a sufficient basis for a search.

[2] Attachment B to the application for a search warrant, which ostensibly tried to particularize the request, contained the following lengthy "list of items to be searched and seized":

> 1. Documents and computer files **in any form** . . . related to or associated with the screen nicknames rubico and rubico10, the e-mail accounts rubico@yahoo.com and rubico10@yahoo.com, dkrocket@mindpsring.com, gov.palin@yahoo.com; Governor Sarah Palin; Facebook, **other internet accounts or online services or groups or hacking activities**.
>
> 6. Computer equipment to include **but not limited to**, central processing units (CPUs), laptops, personal digital assistants, digital media players, cellular phones with digital storage capability, monitors, printers, scanners, pointing devices, cable modems, and software programs relating to or having the ability to connect to the Internet to transmit information. All data processing hardware, computer(s), computer system(s), laptop(s), equipment having data storage capability and the pictures, photos, videos, writings and information stored therein, computer monitors, video monitors or associated television sets to display computer programs and information; all computer printers or output devices; all computer input devices such as trackballs and mouse devices; all computer programs, software and manuals, documentation, all written literature, printouts, magnetic tapes, **including but not limited** to tape storage devices, floppy storage disks, hard drives, compact disks, tapes, removable drives and disks, and the pictures, photos, videos, writings or information stored therein; computer modems and telephone instruments that could be attached to the computer and/or modem; scanners or other computer devices that are used to generate computer files from printed, photographed or videotaped materials, all of above said items are used as implements or instruments or constitute evidence of the offenses listed in the attached affidavit.
>
> 7. All computer hardware capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting any of the aforementioned records or information in electronic, magnetic or optical formats. Hardware includes any data-processing devices (such as central processing units, memory typewriters, and self-contained laptop or "palm" computers); internal,

removal of these items from Mr. Kernell's apartment was necessary "in order to completely and accurately retrieve data . . . [and] ensure accuracy and completeness of such data," due to the "volume of evidence" contained on computers. (Affidavit ¶ 32). In the affidavit, Agent Fisher acknowledged that "[c]omputer storage devices . . . can store the equivalent of thousands of pages of information," but then stated that "*all* the stored data" must be searched on Mr. Kernell's computer, seemingly without regard to whether there was probable cause to search all of the stored data. (Affidavit ¶ 32(a)) (emphasis added). Agent Fisher did not provide a case-specific justification for the unlimited search, instead relying upon the generalized proposition that "a user *may* seek to conceal criminal evidence by storing it in random order with deceptive file names." Id. (emphasis added).

The affidavit further justified the request for a limitless seizure followed by a limitless search by claiming that it is "difficult to know prior to a search: (1) whether a specific expert or search protocol may be required; (2) if so, which expert may be qualified to analyze the system and its data; and (3) whether and what type of controlled environment may be required."

> external, removable, and peripheral storage devices (such as internal and external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices and media, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, modems, optical readers and digital cameras); and related cables or connections, including cable and wireless network devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).
>
> 8. Any and all instructions or programs stored in the form of electronic or magnetic media which are capable of being interpreted by a computer or related components, including, operating systems, application software, utility programs, computers, interpreters, and any other programs or software used to communicate with computer hardware or peripherals either directly or indirectly, via telephone lines, radio, infrared, cable, or other means of transmission. . . .
>
> 10. Any and all passwords and computer security devices, software, programs, or instructions.
>
> 11. The terms "records", "documents", and "materials", include all of the foregoing items of evidence in whatever form and by whatever means such records, documents, or materials, their drafts, or their modifications may have been created or stored . . . .

Attachment B to Search Warrant.

(Affidavit ¶ 32(b)). The affidavit outlined several factors to consider when determining whether a computer can be analyzed on-site or whether it must be removed. Without applying this analysis to Mr. Kernell's case, Agent Fisher concluded, "[I]t is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized." (Affidavit ¶ 33).

According to the affidavit, it was necessary to search *all* of the stored data to recover "even hidden, erased, compressed, password-protected, or encrypted files." Id. However, the affidavit contained no factual basis for believing that Mr. Kernell hid, erased, compressed, password-protected, or encrypted any files. Similarly, the affidavit contained no facts that would have indicated that Mr. Kernell's computer was vulnerable to "intentional modification or destruction . . . from destructive code imbedded in the system as a 'booby trap'" that could have justified an expansive off-site search. (Affidavit ¶ 32(b)).

The facts cited in the affidavit do not support the generic assumption that crimes involving computers are perpetrated by people who have sophisticated computer skills (and that therefore an extensive off-site search is required). See Maryland v. Garrison, 480 U.S. 79, 84 (1987) (noting that the evidence sought in a warrant is limited by the scope of probable cause to believe that the evidence is on the premises). Even if this were a permissible assumption, it is rebutted by the affidavit's *actual* facts. For example, the affidavit indicates that Mr. Kernell became the government's primary suspect because of a posting made by someone calling himself "rubico" on an internet discussion board, a posting which was allegedly hyperlinked to rubico10@yahoo.com. (Affidavit ¶ 15). It was subsequently "reported throughout the Internet" that this e-mail address was connected to Mr. Kernell, but "Special Agents have been unable to confirm" even the existence of the original hyperlink. (Affidavit ¶ 15). The government trusted

the "rubico posting" enough to make its author a suspect, but the posting's content evinced that rubico had no computer skills beyond the basic ability to navigate the Internet and type queries into search forms on Google and Wikipedia.

The lack of computer skills indicated by the rubico posting excluded the likelihood that the government would find "destructive code" in Mr. Kernell's seized computer, and undermined any justification for an immediate and unlimited off-site search. In the posting, "rubico" described "the story" of what happened with Governor Palin's Yahoo! account, but never claimed or indicated that it required any specialized training or knowledge. On the contrary, "rubico" described how he searched Wikipedia and Google for the answers to the three questions that granted him access to the e-mail account. (Affidavit ¶ 12). No knowledge of computer programming or coding is required to use either Wikipedia or Google. Proof that "rubico" lacked the ability to "booby trap" a computer was evident later in the posting when "rubico" explained that the new password was posted to the discussion board only after nothing was found and only because he did not know how to copy and paste material from an e-mail account onto a filehosting website. (Affidavit ¶ 13).

Finally, the possibility that Mr. Kernell's computer could have been vulnerable to "inadvertent" modification, as stated in the affidavit at paragraph 32(b), could have been addressed without seizing the computer by subjecting it to reasonable conditions to protect access to the property and its use in later proceedings. See Fed. R. Crim. P. 41(g).

II. THE SEARCH EXCEEDED THE SCOPE OF THE WARRANT

The warrant only authorized the seizure of Mr. Kernell's computer hardware and some of his computer files. The warrant did not authorize the wholesale examination of all files on his

computer. Therefore, to the extent that the government has subsequently examined the computer and all of its contents, the government has grossly exceeded the scope of the warrant.

The Fourth Amendment commands that no warrants shall issue except those "particularly describing the place to be searched, and the . . . things to be seized." U.S. Const. amend. IV. The purpose of the particularity requirement is to make "general searches . . . impossible and prevent[] the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192 (1927). See also Andreson v. Maryland, 427 U.S. 463, 480 (1976); United States v. Blakeney, 942 F.2d 1001 (6th Cir. 1991) ("A general order to explore and rummage through a person's belongings is not permitted."). Warrants which contain broad descriptions constitute general exploratory warrants which the Framers intended to prohibit. Here, the warrant stated that government agents were authorized to seize "[d]ocuments and computer files in any form . . . related to or associated with the screen nicknames rubico and rubico10, the e-mail accounts rubico@yahoo.com and rubico10@yahoo.com, dkrocket@mindpsring.com, gov.palin@yahoo.com; Governor Sarah Palin; Facebook, other internet accounts or online services or groups or hacking activities." (Attachment B to Search Warrant). The warrant did not, therefore, permit the wholesale seizure of unrelated, irrelevant, and private documents and computer files. Unrelated computer files for which there was no probable cause are not the "functional equivalent" of computer files for which there was probable cause. Cf. United States v. Word, 806 F.2d 658 (6th Cir. 1986) (defendant's objection to seizure of equivalent materials rejected).

Executing officers are not restricted to seizing *only* named items, but any additional items seized must meet the following test: (1) that the article seized be "of incriminating character and

(2) that it be immediately apparent" to the police that this is so. See Coolidge v. New Hampshire, 403 U.S. 443 (1971). See also Andreson v. Maryland, 427 U.S. 463 (1976) (providing that a court must consider what the executing officers knew about the nature of the crime, its elements, and possible means of proving those elements when determining what unnamed items may be seized as evidence of the crime for which the search warrant issued).

Here, if the government claims that unnamed materials were properly seizable under the Coolidge test, the circumstances surrounding their seizure betray the inapplicability of the test. Nothing was immediately or apparently incriminating; indeed, the warrant requested permission for the computer equipment to be removed and "subsequently processed by a qualified specialist in a laboratory setting." (Affidavit ¶ 32). Materials not covered by the warrant and for which there was no probable cause should not have been seized.

For all other materials, though, the Coolidge test is inapposite, because the excess materials seized from Mr. Kernell were not related to the charges. Rather, the government seized documents and computer files unrelated to the alleged wrongdoing and unmentioned in the warrant because it was easier to seize everything than to seize only those documents and computer files for which they had probable cause. This was unreasonable.

The affidavit admitted that it sought "all stored data to determine which particular files are evidence," implying that some files were unrelated. (Affidavit ¶ 32(a)). It is no justification that it is more convenient for investigators to perform an off-site search than to abide by the Constitution. Limiting procedures could and should have been employed:

> Once computer data is removed from the suspect's control, there is no exigent circumstance or practical reason to permit officers to rummage through all of the stored data regardless of its relevance of its relation to the information specified in the warrant. After law enforcement personnel obtain exclusive control over computer data, requiring them to specify exactly what types of files will be inspected does not present any undue burden. A neutral magistrate should

> determine the conditions and limitations for inspecting large quantities of computer data. A second warrant should be obtained when massive quantities of information are seized, in order to prevent a general rummaging and ensure that the search will extend only to relevant documents.

Winck, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 107 (1994). See also Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 Yale L. & Tech. 120 (2007). That the warrant did not provide for a limiting protocol only means that it was the government's responsibility to evaluate the situation and request a second, particularized warrant to continue their search. Because the government did not sufficiently particularize the original affidavit in support of the search warrant or request a second warrant, even though the investigating agents told the court that computer storage devices "can store the equivalent of thousands of pages of information," (Affidavit ¶ 32) and even though there was no probable cause to seize the majority of these pages of information, the government's agents demonstrably lacked a good faith belief in the propriety of their actions. See Arizona v. Evans, 514 U.S. 1, 12-13 (1995).

In United States v. Beckett, 544 F.Supp.2d 1346 (S.D. Fla. 2008), the defendant argued that the search warrant only permitted the government to seize his computers, not search the files in them. That is not the same as Mr. Kernell's argument. The Beckett Court properly reasoned that:

> Agents are entitled to seize documents if the warrant lists functionally equivalent documents. . . .
>
> Similar evidence not specified in the warrant can still be seized if it had a sufficient nexus to the crime being investigated. . . .
>
> In the instant case, the challenged evidence was otherwise described in the warrant. The agents' affidavit, which was incorporated by reference in the search warrant, went through the forensic computer examination process utilized during a computer search, including searching through all the files on the computer. (GX

11). Agents are not obliged to interpret warrants as narrowly as the Defendant asserts.

Id. 1350-51. Here, then, not only did the warrant incorporate a forensic methodology, but the seized documents were related to the documents listed in the warrant.

Where, as here, the executing agents grossly exceeded the scope of the warrant, the remedy is suppression of all evidence seized pursuant to the warrant. United States v. Medlin, 842 F.2d 1194, 1199 (10th Cir. 1998); United States v. Foster, 100 F.3d 846, 851 (10th Cir. 1996). Convictions are reversed when the scope of the warrant is exceeded. See e.g., Marks v. Clark, 102 F.3d 1012 (9th Cir. 1997) (conviction reversed where warrant to search two residences did not authorize the officers to search all persons present); United States v. Schroeder, 129 F.3d 439 (8th Cir. 1997) (conviction reversed because warrant did not authorize search of adjoining property); see also Leveto v. Lapina, 258 F.3d 156 (3rd Cir. 2001) (holding that warrant for home did not justify pat-down of owner).

III. TO INTERPRET THIS WARRANT TO ALLOW UNLIMITED EXAMINATION OF FILES WOULD TRANSFORM IT INTO AN UNCONSTITUTIONAL GENEAL WARRANT.

If the warrant is interpreted to include both the seizure of hardware and the examination of all of the computer's contents, it is an unconstitutional general warrant. If this Court finds that the forensic searches of Mr. Kernell's computer were authorized by the warrant, because the government seized items for which no probable cause existed – and did so pursuant to the warrant – the warrant was overbroad. The computer seized pursuant to the September 20, 2008 search warrant and all evidence obtained from any subsequent searches of the computer must be suppressed, because the warrant authorized an unconstitutionally broad search and seizure: the list of items to be seized from Mr. Kernell's apartment was insufficiently particularized, both in terms of which items were seized and the permissible scope of any subsequent searches of those

items. Even after seizing more material than that for which there was probable cause to seize, the government did not request approval of a protocol for subsequent searches, and thus one was not established.

The search was unreasonable, in violation of the Fourth Amendment. U.S. Const. amend IV. Although United States v. Ford, 184 F.3d 566, 578 (6th Cir. 1999), provides that the remedy for an overbroad warrant is not to suppress all evidence seized, but rather, "to sever the overbroad portions," here, because the entire warrant was overbroad, all evidence seized and subsequently obtained from a search of the contents must be suppressed.

Intrusion upon one's expectation of privacy in one's premises is limited by precise descriptions, making the particularity requirement for warrants directly related to the probable cause requirement. See Maryland v. Garrison, 480 U.S. 79, 85 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications . . . ."). The less precise the description of the place to be searched or things to be seized, the less likely there is probable cause to seize the enumerated items. For example, if a description is broader than can be justified by the probable cause upon which the warrant is based, the description could be defective. See VonderAhe v. Howland, 508 F.2d 364 (9th Cir. 1974) (finding warrant invalid where government knew what financial records it sought but requested all records relating to the defendant's finances). Generality is permitted when greater specificity is impossible or when the scheme investigated is particularly complex. See Andreson, 427 U.S. at 480 n.10 (complex nature of real estate scheme under investigation must allow for some generality of description). And, although there are instances when an affidavit can establish probable cause that a business is so "permeated with fraud" that virtually all records can be

seized, the affidavit made no attempt to do so in this case. Furthermore, the "permeated with fraud" showing must be made in the affidavit and not by relying on what was actually seized. See United States v. Ford, 184 F.3d 566, 576 (6th Cir. 1999) ("Even if one business carried on at a site is permeated with fraud, if other businesses run at the same site are separable and are not shown to be related to the suspected crime, a warrant permitting seizure of all documents at the site is not justified.").

Here, if electronic rummaging was authorized, the warrant was defective because the discretion of the person searching Mr. Kernell's computer was not limited to searching for those items for which there was probable cause. United States v. Ford, 184 F.3d 566 (6th Cir. 2000) (conviction reversed because search warrant authorized broader search than reasonable); United States v. Kow, 58 F.3d 423 (9th Cir. 1995) (conviction reversed where warrant failed to identify business records with particularity, and good faith exception did not apply); United States v. McGrew, 122 F.3d 847 (9th Cir. 1997) (conviction reversed because search warrant affidavit lacked particularity); In re Grand Jury Investigation, 130 F.3d 853 (9th Cir. 1997) (conviction reversed because search warrant was overbroad).

A. The List of Items to Be Seized Was Unconstitutionally Broad.

If the warrant is read to allow examination of all files at the discretion of law enforcement, the list of items to be seized from Mr. Kernell's apartment lacked sufficient particularization. Rule 41 requires, in part, that, "[T]he warrant must identify the . . . property to be searched, identify any . . . property to be seized, and designate the magistrate judge to whom it must be returned." Fed. R. Crim. P. 41(e)(2)(A).[3] The affidavit outlined several factors to be

[3] The affidavit claims that, "Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentalities, fruits, or evidence of crime; or (2) storage devices for information about crime." (Affidavit ¶ 30). More accurately, Rule 41 only permits a warrant to be issued for:

considered when determining whether a computer can be analyzed on-site or whether it must be removed. However, without applying this analysis to Mr. Kernell's case, Agent Fisher concluded, "[I]t is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized." (Affidavit ¶ 33).

Mr. Kernell's computer and all of its contents were seized. A "seizure" of property is a "meaningful interference with an individual's possessory interests in that property." United States v. Jacobsen, 466 U.S. 109, 113 (1984). The Return indicated that Mr. Kernell's laptop computer was taken pursuant to the warrant. (Return In the matter of the Search of Room A, 3:08-MJ-1084, 9/20/2008). When a computer is seized, its contents are necessarily seized, too. However, the notation that a "laptop computer with power cord" was taken from Mr. Kernell does not accurately convey the amount of information contained within the hard drive which was seized, nor does it differentiate between relevant and unrelated content on the hard drive which was seized.[4] Because the government seized items for which no probable cause existed – and did so pursuant to the warrant – the warrant was overbroad. See United States v. Abboud, 438 F.3d 554 (6th Cir. 2006) ("warrant was overbroad," as it authorized search for records from Jan. 1996 to May 2002, but probable cause shown only as to 3-month period in 1999). But see United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006) (warrant for "any computer equipment" in residence "callable of being used to commit, further, or store evidence of the offense" not too broad); United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982) (noting that probable cause

---

(1) evidence of a crime;
(2) contraband, fruits of crime, or other items illegally possessed;
(3) property designed for use, intended for use, or used in committing a crime; or
(4) a person to be arrested or a person who is unlawfully restrained.

Fed. R. Crim. P. 41(c).

[4] As discussed more fully bellow, if the execution of the warrant is concluded upon the return, it is not clear what will limit the places to be searched on the computer once in the forensic computer analyst's possession.

to seize specific paper files enumerated in warrant does not permit the seizure of commingled innocent files). In United States v. Kow, 58 F.3d 423 (9th Cir. 1995), a warrant authorizing the seizure of all of a corporation's business and financial records and computer hardware and software, without limits on which items in each category could be seized, and without specifying how the items allegedly related to criminal conduct, or specifying a time frame in which the conduct occurred, was invalid as an overly broad "general warrant." The Kow warrant suffered from the same defects as the warrant in this case.

The affidavit contained no allegations that Mr. Kernell had been or was currently engaged in any other criminal activity that would warrant a blanket authorization to search all of the files on his computer. Compare In re Grand Jury Investigation, 130 F.3d 853 (9th Cir. 1997) (seizure excessive where search warrant related to fraud sought all records pertaining to supply of semiconductors to government programs from 1990 to 1995, and vast majority of defendant's business relates to such supply and government provided no rationale for dates chosen) with United States v. Martinelli, 454 F.3d 1300 (11th Cir. 2006) (search warrant properly allowed seizure of "all" business files, as "there were allegations of a 'pervasive scheme' to defraud"); United States v. Smith, 424 F.3d 992 (9th Cir. 2005) (search warrant authorizing seizure of large volume of business records lawful, as affidavit shows "entirety of the businesses . . . are criminal in nature"). As mentioned in the introduction to this motion, the "rubico posting" upon which the government heavily relied indicated that its author was neither a computer expert nor a criminal mastermind.

In United States v. Ford, 184 F.3d 566 (6th Cir. 1999), the Sixth Circuit reversed the defendant's conviction due to an overbroad warrant. The court found that although "[s]ome of the clauses were expressly limited by reference to illegal gambling or bingo," others had no such

limitation. Based on that warrant, the police seized "several file cabinets and eleven boxes of documents." Id. When the defense moved to suppress those documents "on the grounds that if the documents were within the scope of the search warrant, the search warrant was overbroad, and if the search warrant was read narrowly enough to be valid, the documents were not within its scope," the government did not contend that the warrant should be narrowed by construction.

> [A]ccording to the government, the warrant properly permitted seizure of all financial documents in the buildings, whether or not related to the bingo operations in time or subject matter.
>
> The magistrate judge recommended that the warrant be held valid "in view of the complex nature of the investigation, the pervasive presence of fraud, and the inability of the investigating officers to determine more specifically what items would be subject to seizure." The district court conducted a de novo review and held that the affidavit on which the warrant was based "implicitly established" that Ford's organization was "permeated with fraud" and that the warrant was therefore not overbroad, citing United States v. Oloyede, 982 F.2d 133, 141 (4th Cir.1993).

Id. The Ford court acknowledged that it had recently upheld a warrant containing a paragraph with identically broad language, but distinguished the factual context preceding the disputed warrant and rejected the government's argument that a broad seizure was necessary. "This argument would allow virtually unlimited seizure of a lifetime's worth of documentation, which is extremely intrusive." As in Ford, the warrant in this case contained clauses which were not limited to criminal behavior. See Attachment B to Warrant.

Further, the warrant was overbroad because it permitted the government to search and seize "[d]ocuments and computer files any in form [sic] . . . that may [be] related or be associated with . . . internet accounts or online services or groups, or hacking activities." (Attachment B).[5] Because there are at least two stages to the computer search process, including

[5] Although the attachment appears to have limited the seizure to documents and computer files related to "the screen nicknames rubico and rubico10, the e-mail accounts rubico@yahoo.com rubico10@yahoo.com, dkrocket@mindspring.com, gov.palin@yahoo.com; Governor Sarah Palin; [and] Facebook," (Attachment B to

the physical search for the computer hardware and the later electronic search to retrieve specific data, the warrant did not sufficiently limit the discretion of a forensic analyst during a subsequent search. The purpose of seizing a computer, after all, is to further search it. The small physical size of a computer belies the amount of information contained within it. There are no sufficiently valid portions of the attachment which can be severed from the overbroad.

B. The Place to Be Searched Was Unreasonable (Unconstitutionally Broad).

Computers are seized to further search them, but the warrant at issue neither particularly described the places on Mr. Kernell's hard drive to be searched nor specifically indicated the information for which there was probable cause *to* search, effectively permitting government agents to conduct searches of infinite duration and unlimited scope. Consequently, because the warrant did not curb the computer analyst's discretion or prescribe the scope of a permissible search of the computer's contents, the warrant was overbroad.

Mr. Kernell concedes for purposes of this motion only that the government properly obtained a warrant to enter his home and seize his property. See Kyllo v. United States, 533 U.S. 27, 31 (2001). In general, a seizure is limited to the evidence described in the warrant. See Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications). However, although the physical location of Mr. Kernell's apartment was meticulously described, the places on Mr. Kernell's computer were not similarly or sufficiently detailed. Compare Attachment A to Search Warrant with Attachment B to Search Warrant.

Warrant), these words had only superficial effect because they were subsumed under the more general language of the attachment.

The Supreme Court has held that an officer can enter any space not protected by a reasonable expectation of privacy without being counted as a "search." Illinois v. Andreas, 462 U.S. 765, 771 (1983). If an officer wants to enter a non-public place (i.e., a place protected by a reasonable expectation of privacy), he may do so only under special circumstances, see Smith v. Maryland, 442 U.S. 735, 739 (1979),[6] and generally cannot look for evidence in a place smaller than the evidence he wishes to seize. Because electronic data takes up virtually no space, without externally-imposed limits on the scope of a computer search, a forensic analyst has unfettered access to all files.

A computer is similar to a container; under Fourth Amendment jurisprudence, the opening up of a container constitutes a search of its contents. See United States v. Blas, No. 90-CR-152, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990) ("[A]n individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container."). Sifting through the contents of a computer's hard drive and exposing each packet of information is the equivalent of opening a closed container in a house; this constitutes a separate search. See e.g., United States v. Block, 590 U.S. 535, 541 (4th Cir. 1978) (search of footlocker in a room). Probable cause to search some files on a computer does not provide probable cause to search all files. United States v. Ross, 456 U.S. 798, 824 (1982) ("Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable

[6] The plain view doctrine permits the police to seize evidence discovered during a valid search if the incriminating nature of the item to be seized, enough to create probable cause that the item constitutes evidence, is readily and immediately apparent. This doctrine cannot cure the unconstitutionality of this search and seizure. A government agent must have a right to be present at the time the evidence is in "plain view." Coolidge v. New Hampshire, 403 U.S. 443 (1971); United States v. Calloway, 116 F.3d 1129 (6th Cir. 1997). The government may not employ an electronic device to obtain information in an area where one has a reasonable expectation of privacy that could not be gained through sensory observation. See United States v. Karo, 468 U.S. 705, 715 (1984); United States v. Knotts, 460 U.S. 276 (1983).

cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab."). If one has a reasonable expectation of privacy in a container's contents, a search violates that privacy expectation. United States v. Ross, 456 U.S. 798 (1982). Granted, the traditional understanding of the scope of the Fourth Amendment's protections is complicated by the technology involved, but the basic premise remains the same: needle-in-the-haystack searches are unsupportable under the Fourth Amendment without probable cause.

The warrant did not prevent an invasive search of private information because it placed no limits on the analyst. For example, though the government was concerned with events occurring on or about September 16-17, 2008, neither the warrant nor the affidavit suggested a timeframe to curb the scope of the search. See United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) (suggesting in *dicta* that agents executing a search for computer files "could have at least checked the date on which each file was created, and avoided copying those files that were created before the time period covered by the warrant"). Similarly, no time limit was placed on the duration of searches of Mr. Kernell's computer. Nothing in the warrant prevents the repeated and prolonged search of Mr. Kernell's computer.

In United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005), the Tenth Circuit explained the application of the particularity requirement in the context of computer searches and quoted from an earlier opinion which reasoned that:

> [O]fficers conducting searches (and the magistrates issuing warrants for those searches) cannot simply conduct a sweeping, comprehensive search of a computer's hard drive. Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the "intermingling" of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.... Thus, when officers come across computer files intermingled with irrelevant computer files, they may seal or hold the computer pending approval by a magistrate of the conditions and limitations

> on a further search of the computer.... Officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant.

United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005) (quoting United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001)). Because of the intermingling problem, the Tenth Circuit concluded that, "[W]arrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material." Id.

Mr. Kernell respectfully submits that the search warrant, the affidavit, and/or any of the attachments should have specifically stated which terms could be searched on the computer and the methodology for searching for them. The Department of Justice appears to agree that this is the best practice. In the Department's own manual, it is suggested that "[w]hen agents have a factual basis for believing that they can locate the evidence using a specific set of techniques, the affidavit should explain the techniques that the agents plan to use to distinguish incriminating documents from comingled documents." Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 73 (July 2002) available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (last visited Jan. 6, 2009). Some federal courts properly require this practice. See In re Search of 3817 W. West End, First Floor Chicago, Illinois, 60621, 321 F. Supp. 2d 953 (N.D. Ill. 2004) (magistrate judge refused to issue a warrant without a search protocol settled beforehand); United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930 (D. Utah Apr. 12, 2001) (suppressing evidence in absence of search protocol) ("[M]ethods or criteria should have been presented to the magistrate before the issuance of the warrants or to support the issuance of a second, more specific warrant once intermingled documents were discovered.").

The warrant lacked both a limiting search methodology and a particularization of the places on the computer to be searched. As such, the warrant was executed like a general exploratory warrant, contrary to the Fourth Amendment. Cf. United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) ("By its terms, the warrant thus permitted the officers to search for anything – from child pornography to tax returns to private correspondence."); United States v. Carey, 172 F.3d 1268, 1273 n.4 (10th Cir. 1999) (warrant authorizing search of suspect's computer for files pertaining to sale or distribution of controlled substances insufficiently particular to justify seizure of child pornography images from closed files on defendant's hard drive). But see United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005) (search warrant for computer search, including for "electronic files," not overbroad when limited to "evidence of child pornography").

Here, the affidavit and warrant should have prescribed a search strategy for the forensic specialist to follow in order to limit the scope of the search, as discussed in Section II. See Winck, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 107 (1994); Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 Yale L. & Tech. 120 (2007); United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999) (concluding that because the detective "exceeded the scope of the warrant," the "seizure of the evidence upon which the charge of conviction was based was a consequence of an unconstitutional general search, and the district court erred by refusing to suppress it").[7] Technology exists which could

[7] [B]ecause this case involves images stored in a computer, the file cabinet analogy may be inadequate. "Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information." Relying on analogies to closed containers or file cabinets may lead courts to "oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage." *Id.* Alternatively, courts can acknowledge computers often contain "intermingled documents." Under this approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search

have easily limited the government's intrusion into places on the computer for which there was no probable cause to search. For example, the government could have run an on-site forensic software program in the hopes of establishing probable cause to support an application for a warrant to further search the computer; or, the government could have made a mirror-image of the hard-drive, and then limited its search terms to those terms and dates for which probable cause existed, and then made another application to the court for permission to further search the computer.

If unfeasible pre-seizure, once seized, there were no exigent circumstances which would have prevented law enforcement from presenting a plan to a neutral magistrate. Some Sixth Circuit precedent appears to hold the contrary.

> The warrant authorized the seizure of personal communications related to the offense. Although there were presumably communications on the computers that did not relate to the offenses, "[a] search does not become invalid merely because some items not covered by a warrant are seized." . . . Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files.

Guest v. Leis, 255 F.3d 325, 334-35 (6th Cir. 2001). This case is distinguishable from Mr. Kernell's case and the search and seizure of his computer and its files. As discussed more fully

---

> through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought.
>
> Because in Mr. Carey's case, officers had removed the computers from his control, there was no "exigent circumstance or practical reason to permit officers to rummage through all of the stored data regardless of its relevance or its relation to the information specified in the warrant." With the computers and data in their custody, law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory. *See id.* at 107. In this case, Detective Lewis and the computer technician did list files on the directory and also performed a key word search, but they did not use the information gained to limit their search to items specified in the warrant, nor did they obtain a new warrant authorizing a search for child pornography.

United States v. Carey, 172 F.3d 1268, 1275-76 (10th Cir. 1999).

in the introduction to this motion, (1) there were no allegations that Mr. Kernell had been or was currently engaged in any other criminal activity that warranted a blanket authorization to search all of the files on his computer, and (2) the "rubico posting" which formed the basis for the government's interest in Mr. Kernell indicated a lack of sophisticated computer skills. It would not have been unreasonable for the government to perform a limited search of Mr. Kernell's computer on-site, limited to the bounds of probable cause, followed by a second warrant containing a more particularized request for a limited search. Because the government did not attempt to separate relevant from irrelevant files, the results of all overbroad and invasive searching should be suppressed.

IV. CONCLUSION

Because the warrant did not authorize the government to conduct a forensic analysis of the entire computer and materials for which there was no probable cause, the execution of the warrant exceeded the permissible scope of the search. All evidence obtained outside the scope of the warrant and for which there was no probable cause should be suppressed. If the warrant is interpreted to have permitted a search of all of the computer's contents, because no protocol was specified and no limitations were placed on the executing or analyzing agent's searches of the computer, the warrant was overbroad and invaded Mr. Kernell's reasonable expectation of privacy. The warrant's lack of particularization permitted violations of the Fourth Amendment and the good faith exception does not apply, requiring that all evidence obtained must be suppressed.

Respectfully submitted this 9th day of January, 2009.

RITCHIE, DILLARD & DAVIES, P.C.

/s/ WADE V. DAVIES

WADE V. DAVIES [BPR #016052]
ANNE E. PASSINO [BPR #027456]
606 W. Main Street, Suite 300
P. O. Box 1126
Knoxville, TN 37901-1126
(865) 637-0661

Counsel for David C. Kernell

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and exact copy of the foregoing has been filed electronically this 9th day of January, 2009. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. Parties may access this filing through the Court's electronic filing system.

/s/ Wade V. Davies
WADE V. DAVIES